
NOTE

WHO CONTROLS THE INTERNET? STATES' RIGHTS AND THE REAWAKENING OF THE DORMANT COMMERCE CLAUSE

ARI LANIN^{*†}

INTRODUCTION

The Internet¹ has permanently and unmistakably changed the face of commerce. While legislators have been trying to determine how existing law can be practically applied to the Internet, lawyers and legal scholars realize why it cannot. The inability to apply existing law elegantly to the Internet has prompted a sea of legislation specifically drafted to traverse the cyberspace age. These new and anticipated regulations have, in turn, caused a literal resurrection of the Dormant Commerce Clause. The Internet has brought to life once again the vexing question of whether a state law impermissibly burdens interstate commerce.

* I dedicate this Note to my mother, Arline Lanin, as a symbol of my appreciation for all the time, energy, and love she has invested and continues to invest in me. I value tremendously everything she has done for me—her caring, her persistence, her effort, and, of course, the countless nights she stayed up to make sure I finished my school work. Her interest in my well-being means more to me than she could ever understand. If it had not been for her constant attention, I would not be where I am today.

† I would like to thank Professor Shapiro for his help on this Note and for his invaluable assistance both within and outside of my Constitutional Law class. If it had not been for the time and patience he put into our conversations and e-mail correspondence, I would never have the understanding of the presented material that I do today. Thanks also to Sandeep Motwani for his endless editing help.

1. "Internet" is short for interconnected network.

The purpose of this Note is to explore the effect the dormant aspect of the Commerce Clause has on various types of state regulations, and to discover which types of state laws can and cannot be expected to survive in the future. In the final analysis, it will reveal that states have very little leeway to control the Internet and Internet-related activities, as the Internet is a creature that lives and breathes within the realm of interstate commerce, and thus within the domain of the federal government.

Part I of this Note looks at the nature and history of the Internet. This section briefly explains the Internet's origins, evolution and characteristics. It is intended to give the reader a solid foundation for the analysis that lies ahead, and it presents the distinguishing characteristics of the Internet. Part II exposes the framework of the Dormant Commerce Clause. In Part III, this Note demonstrates that states can regulate very few aspects of the Internet without impermissibly burdening interstate commerce. This section uses a Dormant Commerce Clause analysis of various types of state legislation, including regulations of obscenity, gambling, unsolicited electronic mail, and other commercial transactions. Finally, in Part IV, this Note briefly examines state laws relating to Internet Service Providers, and at the same time presents a partial solution to the Dormant Commerce Clause problem.

I. THE HISTORY AND NATURE OF THE INTERNET

Understanding the unparalleled history of the Internet is essential to appreciate the novel technological, intellectual, and legal issues that it presents. The Internet is a true innovation; it has grown faster and richer than any previous medium of communication. As a result of its unprecedented form and evolution, the Internet cannot, as a whole, be properly analogized to any communications medium that has preceded it.

The Internet's humble beginnings can be traced back to the Cold War anxiety of the United States government. Its original purpose was to use what were then prohibitively expensive² computers more efficiently and to create a national communications network that would be less susceptible to a nuclear attack.³ In 1958, the Advanced Research Projects Agency

2. See Edward A. Morse, *State Taxation of Internet Commerce: Something New Under the Sun?*, 30 CREIGHTON L. REV. 1113, 1118 (1997) (explaining that computers at this time ranged in cost from \$500,000 to more than \$1,000,000 each).

3. See KATIE HAFNER & MATTHEW LYON, *WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET* 41, 59 (1996).

("ARPA")⁴ was created as a hub for sophisticated technological and computer research.⁵ Soon thereafter, a director at ARPA realized that linking computers together would reduce inefficiencies⁶ and allow for the amalgamation of the ideas of many researchers.⁷

The first network, ARPANET, was initially intended only to connect a relatively small number of host computers.⁸ However, ARPANET (ultimately referred to as "the Net") grew at an extraordinarily rapid pace, and by 1972 it consisted of twenty-nine different host computers, most of which were located at universities.⁹ ARPANET showcased the advent of three truly unique and distinctive features that distinguished it from other means of communication. These features are still present in the Internet of today: (1) a distributed network (or "smart networking"), (2) segmented messages,¹⁰ and (3) Transmission Control Protocol/Internet Protocol ("TCP/IP").¹¹

A distributed network ("smart networking") refers to the spider-web-like design of interconnected stand-alone computers. Each computer on the Internet is connected to a small number of other computers. If one information route is down or congested, smart networking allows for information to take any number of alternative routes.¹²

4. See *id.* at 11–13 (ARPA had been heavily involved in funding cutting-edge computing research at various academic and research facilities across the country).

5. See *id.* at 20.

6. See *id.* at 12–13. At this time, intense computer development competition caused manufacturers of computers to write proprietary operating systems so that programs written for different computers were not interchangeable. Thus, not only was it necessary for documents to be duplicated for different research projects, it was necessary to duplicate various data for different operating systems.

7. See *id.* at 41.

8. See David S. Prebut, *State and Local Taxation of Electronic Commerce: The Forging of Cyberspace Tax Policy*, 24 RUTGERS COMPUTER & TECH. L.J. 345, 347 (1998).

9. See Morse, *supra* note 2, at 1119.

10. See HAFNER & LYON, *supra* note 3, at 59–60. The idea of segmented messages later became known as "packet switching." See *infra* notes 13–14 and accompanying text.

11. See Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts & Stephen Wolff, *A Brief History of the Internet* (last revised Apr. 14, 2000) <<http://www.isoc.org/internet-history/brief.html>>; *infra* notes 15–16 and accompanying text.

12. The relevance of smart networking can be seen through a simple example. Imagine a five-tiered pyramid of computers. On the bottom level there is only one computer, on the second level three, on the third level five, on the fourth level seven, and on the fifth level nine. Also, imagine that each computer on one level is connected to one or two other computers at that level, and to only one computer on a higher level. If a computer on level one attempts to communicate with a computer on level five, as long as the computer on level one can communicate with any computer on level two, multiple lines of communication would have to be down for that line of communication to be broken.

Segmented messages ensure that a single message will never be sent in a single block, but instead will be broken down into smaller blocks known as “packets.”¹³ When a message is sent, these “packets” are individually transferred and, inevitably, distributed through different routes on the network. When all the packets arrive at the destination computer, they are reassembled into the original message.¹⁴

TCP/IP is a system of global computer addressing that assigns computers numeric network addresses. This method of addressing has no true relation to geographical location.¹⁵ The use of TCP/IP, task computers called “gateways,” and “routers,” which provide dedicated links between networks, allow different computers to communicate through various networks. This, in turn, gives computers the illusion of being connected to the same virtual network.¹⁶

In 1989, the face of the Internet changed forever. Tim Berners-Lee, of the Switzerland CERN atomic research center,¹⁷ proposed a method of using the now well-known concept of a graphical user interface¹⁸ to browse through Internet-based documents using a mouse.¹⁹ His invention, called hypertext markup language (“HTML”), allowed users to click on “hyperlinks,” which instruct the computer to load different documents from any networked computer. Because it allowed programmers to reference other documents internally rather than requiring separate downloading of individual ones, HTML provided for seamless access to documents located on computers all over the world. The introduction and circulation of web-browsing²⁰ software in 1993 followed the creation of HTML.²¹ The first

The number of possible lines of communication increases exponentially with the addition of levels and the addition of computers to each level.

13. See Prebut, *supra* note 8, at n.10.

14. There are basically two types of electronic communications networks: circuit-switched and packet-switched. Circuit-switched networks are based on dedicating a connection between a sender and a recipient. Such a system of dedicated circuits is used for telephones, where it is better not to have any exchange interrupted. See Morse, *supra* note 2, at 1120–21.

15. Thus, a computer with an “IP address” of 128.63.2.40 could be a computer in California or a computer in Boston.

16. See HAFNER & LYON, *supra* note 3, at 246–54. By “virtual network,” I mean that all the computers seem to be working with and running among each other.

17. See J. Neil Weintraut, *Introduction to ROBERT H. REID, ARCHITECTS OF THE WEB: 1,000 DAYS THAT BUILT THE FUTURE OF BUSINESS* xxiii (1997).

18. A graphical user interface (“GUI”) is a rasterized display of iconographic or pictorial symbols and objects typically manipulated on-screen by a pointer controlled by a pointing device such as a mouse or trackball. Conversation with Nathan Raymond (Feb. 21, 1999).

19. See Weintraut, *supra* note 17, at xxiv.

20. Web browsing is the process by which a computer user connected to the Internet may view hypertext information presented in “pages” of content, and call up other “pages” through links embedded in the hypertext.

widely dispersed web browser was called Mosaic.²² Mosaic was more stable than previous browsers and allowed for the incorporation of images within documents written in HTML. Its user-friendly interface and wide dissemination triggered a newfound and commercially marketable interest in the Internet.

Largely because of these distinguishing characteristics, the Internet has grown to become a content medium with no parallel in the history of human communication. “[It] is [now] a decentralized, global communications medium linking people, institutions, corporations, and governments all across the world.”²³ It provides millions of people all over the world with the opportunity to distribute and exchange speech, music, video images, data, and other information with a virtually limitless audience. As of mid-1997, “the Internet was comprised of 56.2 million host computers and almost 9.6 million Web sites in over 171 countries. These numbers are growing exponentially every year.”²⁴ It is estimated that, at present, between 130 million and 304 million people worldwide have access to the Internet.²⁵ Over 3 million stock traders traded 120 billion dollars over the Internet in 1997.²⁶ By the end of 2000, revenues from Internet access and online services are projected to reach between 7 and 10 billion dollars, and online mail-order sales of tangible property²⁷ are projected to reach 6.6 billion dollars.²⁸ Perhaps the District Court for the Eastern District of Pennsylvania said it best when it observed that “the content on the Internet is as diverse as human thought,”²⁹ leading to the conclusion that there is no end in sight to its growth.

It has been suggested that Internet communication differs fundamentally from more traditional forms of communication such as

21. See Weintraut, *supra* note 17, at xxiv.

22. See *id.* at xxiii–xxiv. Mosaic was distributed for UNIX, Windows 3.1 and Macintosh operating systems.

23. American Libraries Ass’n v. Pataki, 969 F. Supp. 160, 164 (S.D.N.Y. 1997).

24. Mitchell P. Goldstein, *Service Provider Liability for Acts Committed by Users: What You Don’t Know Can Hurt You*, 18 J. MARSHALL J. COMPUTER & INFO. L. 591, 593 (2000) (citation omitted).

25. See *id.*

26. See Michael A. Geist, *The Reality of Bytes: Regulating Economic Activity on the Age of the Internet*, 73 WASH. L. REV. 521, 523 (1998).

27. This figure does not include property acquired by online data transfer.

28. See Leiner et al., *supra* note 11.

29. ACLU v. Reno, 929 F. Supp. 824, 842 (E.D. Pa. 1996).

radio, television and print media in four respects: (1) accessibility, (2) anonymity, (3) transience, and (4) interactivity.³⁰

The Internet is far more accessible than other forms of communication in that virtually anyone can obtain access. Connected users can take advantage of the Internet in a myriad of different ways. Schools often provide Internet accounts to students and faculty, and employers are increasingly furnishing accounts to their employees. People in certain communities can access the Internet via a community network or a local library that provides direct or modem access to its patrons. Even computer coffee shops ("Internet cafes") offer access to the Internet. Of course, anyone who does not fit into the preceding groups can, with a reasonably up-to-date computer, a modem, and an Internet Service Provider ("ISP"), or online service,³¹ utilize the full spectrum of resources available on the Internet.

Particularly notable is the practical anonymity Internet users and hosts enjoy.³² Each IP address,³³ which indicates a computer's numerical name on the network, is given a logical address, such as "www.southerncalifornia.com." This address may provide little or no information about the physical and geographic location of the host computer. Therefore, a web site with the name "www.southerncalifornia.com" actually may be on a server computer in New Jersey and a mirror³⁴ computer in Nevada, while leading everyone who accesses the site to believe that it is actually maintained in California.³⁵ The result is that a user will not likely be able to tell which server is handling its transaction or where that server is. Conversely, the server may not be able to tell who the user is, or where the user is physically located. A host computer, moreover, has little way of knowing who is logging on to its site. Although Web sites are generally accessed anonymously, some web sites require users to log in and give a password. In situations where a username is required, it may be of no value whatsoever in identifying a user, as "[m]any

30. See Patrick Weston, Case Note, *American Civil Liberties Union of Georgia v. Miller*, 14 BERKELEY TECH. L.J. 403, 408 (1999).

31. Examples of online services are America Online, CompuServe, Prodigy and the Microsoft Network.

32. See Weston, *supra* note 30, at 408-10.

33. See *supra* note 15 and accompanying text.

34. Redundancy is often built into these sites as host computers often have at least one other "mirror" server which may be located in another part of the country or another part of the world. See Peter A. Glicklich, Sanford H. Goldberg, & Howard J. Levine, *Internet Sales Pose International Tax Challenges*, 84 J. TAX'N 325, 325 (1996).

35. See Kenneth D. Bassinger, Note, *Dormant Commerce Clause Limits on State Regulation of the Internet: The Transportation Analogy*, 32 GA. L. REV. 889, 908-10 (1998).

usernames are pseudonyms, known as 'handles,' which provide users with a distinct online identity [but] preserve anonymity."³⁶

A third inherent characteristic of Internet communication is transience.³⁷ "When traveling the Internet, we receive little or no warning as to when we have left our state or indeed the nation; it is an international communications medium with no recognizable borders."³⁸ As explained above, because the Internet makes use of smart networking,³⁹ similar information that travels over the Internet may take a variety of different routes. "While a sale of goods to a resident of Los Angeles off the home page of a Boston-based company may travel through eight states and five computers, minutes later a similar transaction may travel through six states and nine computers, or even possibly through another country or over a satellite."⁴⁰ Moreover, the concept of packet switching⁴¹ means that different pieces of any given communication may have taken different courses before arriving at the intended destination. Thus, a portion of the transmission involving the above sale of goods may have gone through four states and another portion may have gone through five. "Conceivably, one single picture may travel through several states with only small pieces of it passing through any one state on its way to being reassembled at the destination computer."⁴² The practical import of all of this is that while an Internet transaction is taking place, it is practically impossible geographically to locate the ingress and egress of the transmission. After an Internet transaction has already taken place, there is no way to know where it passed through and whether each part of it passed through the same place.

The Internet also provides for the utmost in interactive communication.⁴³ Communications on the Internet can occur almost instantaneously, and they can be directed to specific individuals, to a broader group of people interested in a particular subject, or to the world as a whole. These communications take a variety of forms including file transfer protocol ("FTP"), Gopher, Internet Relay Chat ("IRC"), the World Wide Web ("WWW"), USENET newsgroups, telnet, mail exploders,

36. *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 165 (S.D.N.Y. 1997).

37. *See* Weston, *supra* note 30, at 408, 410–11.

38. H. Joseph Hameline & William Miles, *The Dormant Commerce Clause Meets the Internet*, BOSTON B.J., Sept.–Oct. 1997, at 8, 8.

39. *See supra* note 12 and accompanying text.

40. Hameline & Miles, *supra* note 38, at 8.

41. *See supra* text accompanying notes 13–14.

42. Bassinger, *supra* note 35, at 894.

43. *See* Weston, *supra* note 30, at 408, 411.

Internet video, audio conferencing, and perhaps the most-used of all Internet communications means, electronic mail (e-mail). E-mail is the most basic Internet communication, for it involves simply the sending of one message, ostensibly from one computer to another. Mail exploders, USENET newsgroups and chat rooms are the most common means of discussion on the Internet. Mail exploders allow users to subscribe to mailing lists. When other subscribers mail messages to the mailing list, the exploder redirects that message to all of the subscribers.⁴⁴ USENET allows users to read or send messages to newsgroups without any prior subscription. There is no way for a USENET reader to know who any speaker is just by reading the message. IRC allows for discussion between two or more users in a real-time environment, or “room,” which enables users to engage in simultaneous conversations with one or many “occupants” by typing in messages and reading the messages left by others. The most widely used Internet component, the WWW, is truly a publishing forum.⁴⁵ Internet users worldwide can create web pages and view the web pages of others.⁴⁶ These web pages can contain text, graphics, sounds, video clips, and more. An astounding number of companies (both large and small), banks, brokerage houses, newspapers, and magazines provide online editions of their reports and publications.⁴⁷ Government agencies and even courts use the web to disseminate information to the public.⁴⁸ Real-time Internet communication occurs utilizing a full range of multimedia technologies. Users communicate with text, sound, pictures, movies, and Internet “applets.”⁴⁹ “This interactivity makes the Internet ideally suited for electronic commerce. . . .”⁵⁰

II. THE DORMANT COMMERCE CLAUSE—THE STATES’ RIGHT TO CONTROL

A. THE LAW BEFORE THE INTERNET

Article One, Section Eight of the United States Constitution grants Congress the power “To regulate Commerce with foreign Nations, and

44. *See* *Shea v. Reno*, 930 F. Supp. 916, 927 (S.D.N.Y. 1996).

45. *See* *Reno v. ACLU*, 521 U.S. 844, 852–53 (1997).

46. *See id.*

47. *See id.* at 853.

48. *See id.*

49. An applet is a program written in one of several programming languages that can be included in an HTML page, much as an image or a sound file is included.

50. *Weston*, *supra* note 30, at 411.

among the several States . . .”⁵¹ Although no express provision in the Constitution specifically enjoins the states from regulating interstate commerce, as far back as 1824, the Supreme Court found that this “Commerce Clause” implies such a restriction. The Marshall Court, in *Gibbons v. Ogden*, ruled that when a state proceeds to regulate interstate commerce, it is exercising the very power that is granted to the federal government under the Commerce Clause, and thus is doing the very thing which only Congress is authorized to do.⁵² The Supreme Court has used this rationale to prohibit the states from regulating interstate commerce.⁵³ This aspect of the commerce power has come to be known as the “dormant” or “negative” Commerce Clause.

Unfortunately, determining the existence of the Dormant Commerce Clause is the easy part. Because Dormant Commerce Clause jurisprudence is clumsy and incoherent, figuring out how to apply it to any given state law is far more difficult. The Supreme Court’s inability to state a consistent, cogent rule of law concerning the Dormant Commerce Clause over the past 175 years has caused this area of legal scholarship to mushroom into a cloud of confused holdings and inelegantly reasoned opinions. While in some situations the Supreme Court’s Dormant Commerce Clause opinions can be reconciled with one another, in others, reconciliation is impossible.⁵⁴ Owing to the inconsistency of the relevant cases, there is no one static constitutional analysis that provides a simple solution to the question of how to apply the Dormant Commerce Clause. What the Dormant Commerce Clause cases reveal is a level of disagreement that necessitates a full understanding of not only the dicta contained within the text, but of the underlying constitutional principles embodied therein. To further this understanding, one must recognize the kinds of laws the Supreme Court tends to strike down, and the loosely structured analysis that appears to be taking place when those laws are invalidated.

The cases illustrate that the Supreme Court has used the negative implication of the Commerce Clause to prohibit individual states from passing two kinds of laws. First, states may almost never pass laws that openly discriminate against interstate commerce.⁵⁵ In other words, a state

51. U.S. CONST. art. I, § 8.

52. 22 U.S. (1 Wheat.) 1 (1824).

53. See, e.g., *Willson v. Black Bird Creek Marsh Co.*, 27 U.S. (1 Pet.) 245 (1829).

54. Conversation with Michael Shapiro, Professor of Law, University of Southern California Law School (Feb. 1, 1999).

55. See, e.g., *City of Philadelphia v. New Jersey*, 437 U.S. 617, 623–27 (1978).

law that on its face protects or favors in-state economic interests over out-of-state economic interests will almost always be void. For example, in the seminal case of *City of Philadelphia v. New Jersey*, a New Jersey state law that prohibited the import of most “solid or liquid waste which originated or was collected outside the territorial limits of the State,”⁵⁶ was invalidated as violative of the Dormant Commerce Clause.⁵⁷

Second, states may not pass laws that burden interstate commerce disproportionately in relation to intrastate commerce,⁵⁸ whether that burden is intended or not.⁵⁹ The case of *Kassel v. Consolidated Freightways Corp.*⁶⁰ exemplifies this principle. In *Kassel*, an Iowa statute prohibited the use of 65-foot double tractor-trailers on Iowa highways.⁶¹ The law limited use of the highways to 55-foot single tractor-trailers.⁶² The statute, which was enacted for safety reasons, did not discriminate against out-of-state interests on its face.⁶³ Rather, it was a blanket, even-handed prohibition of large trucks used within the state. But because it impacted interstate commerce disproportionately to the local benefit, the Supreme Court invalidated the law.⁶⁴ Iowa’s law would force out-of-state trucking companies to switch truck sizes when traveling through Iowa, adding about \$12.6 million each year to the costs borne by out-of-state trucking companies.⁶⁵ Moreover, the resulting local benefit of the law turned out to be nonexistent. Though research did show that the decrease in tractor-trailer size would reduce the severity of accidents, research also showed that the decrease in trailer size would increase the number of accidents because the use of smaller trucks would require the use of more trucks—and more trucks would lead to more accidents.⁶⁶ Therefore, in *Kassel*, the Supreme Court used the Dormant Commerce Clause to invalidate a law that imposed an unintended disproportionate burden on interstate commerce even though the law was not facially discriminatory.

In considering the constitutionality of these two kinds of laws, courts seem to conform to the following analysis. If a state law is a protectionist

56. *Id.* at 618.

57. *See id.* at 628.

58. *See Pike v. Bruce Church, Inc.*, 397 U.S. 137 (1970).

59. *See Bibb v. Navajo Freight Lines, Inc.*, 359 U.S. 520 (1959).

60. 450 U.S. 662 (1981).

61. *Id.* at 665.

62. *See id.*

63. *See id.* at 667–70.

64. *See id.* at 671.

65. *See id.* at 674.

66. *See id.* at 674–75.

measure by its terms, it is “virtually *per se*” invalid,⁶⁷ and almost always struck down. In other words, to the extent a law states that it is protecting local economic interests at the expense of out-of-state economic interests, it is almost always invalid. Such laws are extremely rare, and will not be considered in this Note. If the law is not a protectionist measure on its face, courts next question whether it discriminates against interstate commerce on its face. Laws that facially discriminated against interstate commerce were at issue in *Dean Milk Co. v. City of Madison*⁶⁸ and *City of Philadelphia v. New Jersey*.⁶⁹ In *Dean Milk*, an ordinance barred the sale of milk not bottled within the state,⁷⁰ and in *Philadelphia v. New Jersey*, discussed above, a state law prohibited the importation of out-of-state waste into New Jersey.⁷¹ If the law is found to be facially discriminatory (as in *Dean Milk* and *Philadelphia v. New Jersey*), courts generally seem to apply a presumption that the law was enacted to fulfill a protectionist purpose.⁷²

To overcome this presumption, the state must show that the law furthers a legitimate state interest.⁷³ This analysis depends in part on such factors as (1) whether the state had a less discriminatory alternative than to enact this particular law; (2) arguments contained in the legislative record; and (3) whether there is an excessive or disproportionate impact on out-of-state interests in relation to in-state interests.⁷⁴ If the conclusion at this point is that a legitimate state interest exists that is the dominant interest in enacting the law, the final inquiry, known as the *Pike* Balancing Test, becomes a cost-benefit analysis of whether the quantitative burden imposed by the law is excessive in relation to the putative local benefit.⁷⁵ If the burden outweighs the benefit, the law is unconstitutional and struck down as an offense against the Commerce Clause. This balancing considers the legitimacy and weight of the state’s interest, whether or not a less discriminatory alternative to the act existed, and the size and type of the disproportion. If the law is not discriminatory on its face, much the same analysis occurs, but without the presumption of protectionism.⁷⁶ Finally,

67. *City of Philadelphia v. New Jersey*, 437 U.S. 617, 624 (1978).

68. 340 U.S. 349 (1951).

69. 437 U.S. 617 (1978).

70. *Dean Milk*, 340 U.S. at 350.

71. *Philadelphia v. New Jersey*, 437 U.S. at 618.

72. *E.g., id.* at 617; *Dean Milk*, 340 U.S. at 353.

73. *See, e.g., Philadelphia v. New Jersey*, 437 U.S. at 628–29.

74. *See Maine v. Taylor*, 477 U.S. 131, 138–40 (1986).

75. *Pike v. Bruce Church, Inc.*, 397 U.S. 137, 142 (1970).

76. Note that the Supreme Court has held that the Dormant Commerce Clause is equally applicable to activities undertaken without a profit motive. *See Edwards v. California*, 314 U.S. 160

the Supreme Court has held that those aspects of commerce that require consistent treatment may not be regulated by the states independently, as such regulations also offend the Commerce Clause.⁷⁷

Even if a state law violates the dormant aspect of the Commerce Clause under the above formula, it can still escape invalidation under the Market Participation Exception.⁷⁸ The Supreme Court set aside a specific exception to the dormant aspect of the Commerce Clause for situations where the state is actually a market participant rather than a market regulator. In *Reeves, Inc. v. Stake*, the Court upheld a South Dakota policy of restricting the sale of state-owned cement to state residents.⁷⁹ The Court held that if a state is acting as a participant in the transaction rather than a market regulator, the Dormant Commerce Clause places practically no limitation on its activities.⁸⁰

B. THE LAW OF THE INTERNET: *AMERICAN LIBRARIES ASS'N V. PATAKI*

Only two cases have actually applied Dormant Commerce Clause analysis to a state's Internet commerce regulation. The seminal case is *American Libraries Ass'n v. Pataki*.⁸¹ There the act in question was an amendment to New York Penal Law section 235.21 that made it a crime for an individual, "knowing the character and content of [a] communication which, in whole or in part, depicts actual or simulated nudity, sexual conduct or sadomasochistic abuse, and which is harmful to minors," to "intentionally use any computer communication system allowing the input, output, examination or transfer, of computer data or computer programs from one computer to another, to initiate or engage in such communication with a person who is a minor. . . ."⁸²

(1941) (holding unconstitutional a statute prohibiting transport of nonresident "indigent persons" into California).

77. See, e.g., *Wabash, Saint Louis & Pac. Ry. v. Illinois*, 118 U.S. 557, 574 (1886) (noting that "the transportation and exchange of commodities is of national importance and admits and requires uniformity of regulation" (quoting *Welton v. Missouri*, 91 U.S. 275, 280 (1875))).

78. See generally *South-Central Timber Dev., Inc. v. Wunnicke*, 467 U.S. 82 (1984); *Reeves, Inc. v. Stake*, 447 U.S. 429 (1980).

79. 447 U.S. 429, 440-47 (1980).

80. *Id.* at 436, 440. Note, however, that under the *South-Central Timber* "market participant doctrine," a state may impose burdens on commerce within the market in which it is a participant, but it may not impose burdens on other or downstream markets. See *Hughes v. Alexandria Scrap Corp.*, 426 U.S. 794, 804-06 (1976).

81. 969 F. Supp. 160 (S.D.N.Y. 1997).

82. N.Y. PENAL LAW § 235.21 (McKinney 1999).

Judge Preska, writing for the District Court for the Southern District of New York, began her examination of whether Dormant Commerce Clause scrutiny was warranted by investigating whether the Act applied to both intrastate and interstate transmissions.⁸³ By its terms, the Act made no distinction between intra- and interstate commerce.⁸⁴ Preska then looked to the Act's legislative history, stating that the record revealed the legislature's understanding to be that the law would apply to communications made between New Yorkers and non-New Yorkers, as well as purely intrastate communications.⁸⁵ She stated, "[t]he conclusion that the Act must apply to interstate as well as intrastate communications receive[d] perhaps its strongest support from the nature of the Internet itself."⁸⁶ Bringing up issues such as anonymity, packet switching,⁸⁷ and smart networking,⁸⁸ Preska came to the conclusion that the Act could not "effectively be limited to purely intrastate communications over the Internet because no such communications exist."⁸⁹ The court went on to state:

No user could avoid liability under the New York Act simply by directing his or her communications elsewhere, given that there is no feasible way to preclude New Yorkers from accessing a Web site, receiving a mail exploder message or a newsgroup posting, or participating in a chat room. Similarly, a user has no way to ensure that an e-mail does not pass through New York even if the ultimate recipient is not located there, or that a message never leaves New York even if both sender and recipient are located there.⁹⁰

Loosely analogizing the Internet to trains⁹¹ and highway travel,⁹² Judge Preska ultimately came to "[t]he inescapable conclusion . . . that the Internet represents an instrument of interstate commerce, albeit an

83. See *Pataki*, 969 F. Supp. at 169–73.

84. See *id.* at 169–70.

85. The court, after citing the legislative record, concluded, "[o]bviously. . . the Act would be completely ineffective in forestalling a pedophile like [petitioner] if it applied only to purely intrastate communications." *Id.* at 170.

86. *Id.* at 170.

87. See *supra* text accompanying notes 13–14.

88. See *supra* note 12 and accompanying text.

89. *Pataki*, 969 F. Supp. at 171.

90. *Id.*

91. See *Southern Pac. Co. v. Arizona ex rel. Sullivan*, 325 U.S. 761, 763, 781 (1945) (Arizona Train Limit Law limiting passenger trains to fourteen cars and freight trains to seventy cars found unconstitutional).

92. See *Kassel v. Consolidated Freightways Corp.*, 450 U.S. 662, 665, 671 (1981) (holding unconstitutional an Iowa statute restricting the length of vehicles that could be used on state highways).

innovative one.”⁹³ Thus, Dormant Commerce Clause scrutiny was appropriate.

After deciding to apply Dormant Commerce Clause scrutiny, Judge Preska studied the Act to determine whether it had offended the bounds of the Dormant Commerce Clause. She found that

[t]he nature of the Internet [made] it impossible to restrict the effects of the New York Act to conduct occurring within New York. An Internet user may not intend that a message be accessible to New Yorkers, but lacks the ability to prevent New Yorkers from visiting a particular Website or viewing a particular newsgroup posting or receiving a particular mail exploder. Thus, conduct that may be legal in the state in which the user acts can subject the user to prosecution in New York and thus subordinate the user’s home state’s policy. . . .⁹⁴

Therefore, “New York ha[d] deliberately imposed its legislation on the Internet and, by doing so, projected its law into other states whose citizens use the Net.”⁹⁵ Preska went on to hold that this type of behavior was per se violative of the Dormant Commerce Clause.⁹⁶

It is here that Preska’s Dormant Commerce Clause scrutiny was incorrectly applied. First, the Act was not per se violative of the Dormant Commerce Clause because it was neither protectionist by its terms nor discriminatory by its terms.⁹⁷ Rather, the act regulated even-handedly, prohibiting transmissions originating from outside the state just as much as transmissions originating from inside the state. State laws that do not discriminate on their face are not subject to a “per se” rule of invalidity. Second, even an act that is protectionist on its terms is not “per se” violative of the Dormant Commerce Clause. As the Court stated in *City of Philadelphia v. New Jersey*, in such cases, the law is only “*virtually per se*” invalid.⁹⁸ Though the use of “virtually” in the rule has never been expressly employed by the Supreme Court, it may be have been implicitly

93. *Pataki*, 969 F. Supp. at 173.

94. *Id.* at 177. *See also* *Bigelow v. Virginia*, 421 U.S. 809, 824 (1975) (“A State does not acquire power or supervision over the internal affairs of another State merely because the welfare and health of its own citizens may be affected when they travel to that State.”).

95. *Pataki*, 969 F. Supp. at 177. *See also* *Southern Pac. Co.*, 325 U.S. at 775. (“The practical effect of [a law limiting train lengths] is to control train operations beyond the boundaries of the state exacting it because of the necessity of breaking up and reassembling long trains at the nearest terminal points before entering and after leaving the regulating state.”).

96. *See Pataki*, 969 F. Supp. at 177.

97. *See supra* text accompanying notes 67–72.

98. 437 U.S. at 624 (emphasis added to the word “virtually”).

used in cases involving the Market Participation Exception or cases involving state emergencies,⁹⁹ and should not be carelessly tossed aside.

After claiming to find the Act to be per se violative of the Dormant Commerce Clause, Preska proceeded to what she called the next prong of the inquiry: whether the Act had unduly burdened interstate commerce.¹⁰⁰ She turned her attention to the balancing test pronounced in *Pike v. Bruce Church, Inc.*—whether the quantitative burden imposed by the law was excessive in relation to the putative local benefit.¹⁰¹ While she accepted the proposition that protection of children from obscenity and pedophilia was a legitimate state interest,¹⁰² that interest alone was not enough to overcome the quantitative burden the act would impose on interstate commerce,¹⁰³ since the benefit to be derived from the Act was actually very low.¹⁰⁴ First, the Act could not protect against obscenity originating from outside the United States.¹⁰⁵ Second, the Act only prohibited images on the Internet, and did not bar purely text transmissions.¹⁰⁶ Third, the Act was not aimed at the sale of obscene material over the Internet.¹⁰⁷ Fourth, the Act's usefulness would be limited by the number of cases the State would actually be able to prosecute.¹⁰⁸ On the other hand, Judge Preska found that the burden on interstate commerce would be significant. The New York law would chill online communication by imposing unduly restrictive compliance costs on some Internet users,¹⁰⁹ while scaring others off the

99. See *supra* note 78 and accompanying text.

100. See *Pataki*, 969 F. Supp. at 177.

101. 397 U.S. 137, 142 (1970). "The distinction between direct regulations of interstate commerce, which are subject to a per se rule of invalidation, and indirect regulations subject to the less stringent balancing test has never been sharply defined. In either situation, however, the 'critical consideration is the overall effect of the statute on both local and interstate activity.'" *Pataki*, 969 F. Supp. at 177 n.8 (quoting *Brown-Forman Distillers Corp. v. N.Y. Liquor Auth.*, 476 U.S. 573, 579 (1986) and *Raymond Motor Transp., Inc. v. Rice*, 434 U.S. 429, 440–41 (1978)).

102. See *New York v. Ferber*, 458 U.S. 747, 756–57 (1982) ("It is evident beyond the need for elaboration that a State's interest in 'safeguarding the physical and psychological well-being of a minor' is 'compelling.'") (quoting *Globe Newspaper Co. v. Superior Ct.*, 457 U.S. 596, 607 (1982)).

103. See *Hunt v. Washington State Apple Adver. Comm'n*, 432 U.S. 333, 350 (1977) ("[A] finding that state legislation furthers matters of legitimate local concern, even in the health and consumer protection areas, does not end the inquiry."); *Bibb v. Navajo Freight Lines, Inc.*, 359 U.S. 520, 528 (1959).

104. See *Pataki*, 969 F. Supp. at 178.

105. See *id.*; *ACLU v. Reno*, 929 F. Supp. 824, 882 (E.D. Pa. 1996).

106. This was not the main reason for the Act's failure. If the Act were to regulate text as well, it likely would have failed on the same grounds.

107. The selling of obscene material was also not the principal reason for the Act's failure.

108. Neither did the Act's potential impotence seal its fate. All these reasons weigh against the putative local interest but by no means dispose of the issue.

109. See *Pataki*, 969 F. Supp. at 180; *ACLU v. Reno*, 929 F. Supp. at 855–56. "Many speakers who display arguably indecent content on the Internet must choose between silence and the risk of

Internet altogether.¹¹⁰ Judge Preska thus found that the Act was a violation of the Dormant Commerce Clause because the burden it imposed on interstate commerce far outweighed the state interest in retaining the law.

Judge Preska concluded her excessive burden analysis by turning to the question of inconsistent regulation:¹¹¹

[C]ourts have long recognized that certain types of commerce demand consistent treatment and are therefore susceptible to regulation only on a national level. The Internet represents one of those areas; effective regulation will require national, and more likely global, cooperation. Regulation by any single state can only result in chaos, because at least some states will likely enact laws subjecting Internet users to conflicting obligations. Without the limitation's [sic] imposed by the Commerce Clause, these inconsistent regulatory schemes could paralyze the development of the Internet altogether.¹¹²

Preska noted that New York was not the only state with these problems and was not the only state to have enacted such legislation, for Georgia and Oklahoma had done so as well.¹¹³ Without consistent legislation in this area, state residents would be under an obligation to obey the intricacies and technicalities of every single state's Internet law to avoid prosecution. This, Preska asserted, would be an unacceptable outcome.¹¹⁴

Judge Preska's approach to the Dormant Commerce Clause can be summarized as follows: (1) question whether the law regulates intrastate activities paying particular attention to the text of the statute and the legislative intent in passing the law; (2) question whether the law creates an undue burden on interstate commerce using the *Pike* balancing test; and (3) question whether the law subjects the Internet, a uniquely interstate medium, to inconsistent regulation.

prosecution. . . . [The] defenses are not technologically or economically feasible for most providers." *Id.* at 849.

110. See *Pataki*, 969 F. Supp. at 180; *ACLU v. Reno*, 929 F. Supp. at 863 (holding that individuals, uncertain of the reach of the Communications Decency Act ("CDA"), will undoubtedly "steer far wider of the unlawful zone"). The CDA, which Congress enacted, made lewd and lascivious conduct illegal on the Internet. The Supreme Court determined the CDA was unconstitutional because its overbroad language violated the First Amendment. See *Reno v. ACLU*, 521 U.S. 844, 874-79 (1997).

111. See *supra* text accompanying note 77.

112. *Pataki*, 969 F. Supp. at 181. See *Wabash, St. Louis & Pac. Ry. v. Illinois*, 118 U.S. 557, 574-75 (1886) (citing *County of Mobile v. Kimball*, 102 U.S. 691, 702 (1880)).

113. See *Pataki*, 969 F. Supp. at 182; GA. CODE ANN. § 16-9-93.1 (1999); OKLA. STAT. ANN. tit. 21, §1040.76 (West Supp. 1999).

114. *Pataki*, 969 F. Supp. at 183.

The *Pataki* opinion is important because it was the first to apply the Dormant Commerce Clause to a state's Internet regulation. Courts will likely refer to Judge Preska's opinion until the Supreme Court receives an opportunity to lay down its interpretation of the law. Though for the most part Preska's analysis mirrored the analysis described above, it was not without its flaws.¹¹⁵ Fortunately, Preska's oversights render her opinion somewhat clumsy, but not unusable. So long as its shortcomings are not overlooked, her opinion can be used as yet another of the many manifestations of Dormant Commerce Clause jurisprudence.

III. THE LAW APPLIED TO THE INTERNET: THE AFTERMATH AND PROBABLE AFTERMATH

A. CRIMINAL STATUTES

1. *Obscenity*

a. *New Mexico: the Tenth Circuit's rigid application of American Libraries Ass'n v. Pataki*

The United States Court of Appeals for the Tenth Circuit, in *American Civil Liberties Union v. Johnson*,¹¹⁶ applied Dormant Commerce Clause scrutiny to section 30-37-3.2 of the New Mexico Statutes.¹¹⁷ Like the statute at issue in *Pataki*, section 30-37-3.2 criminalized Internet dissemination of material harmful to minors. The statute stated, "Whoever commits dissemination of material that is harmful to a minor by computer is guilty of a misdemeanor."¹¹⁸ The New Mexico legislature defined "[d]issemination of material harmful to a minor by computer" as follows:

the use of a computer communications system that allows the input, output, examination or transfer of computer data or computer programs from one computer to another, to knowingly and intentionally initiate or engage in communication with a person under eighteen years of age when such communication in whole or in part depicts actual or simulated nudity, sexual intercourse or any other sexual conduct.¹¹⁹

Plaintiffs attacked the statute on both First Amendment and Dormant Commerce Clause grounds. After ruling that plaintiffs' First Amendment

115. See *supra* text accompanying notes 97-99.

116. 194 F.3d 1149 (10th Cir. 1999).

117. N.M. STAT. ANN. § 30-37-3.2 (Michie Supp. 1999).

118. § 30-37-3.2(A).

119. *Id.*

argument showed a sufficient likelihood of success on the merits to justify a preliminary injunction, the court of appeals turned its attention to the Commerce Clause. Though the court did address the Commerce Clause issue, its decision was cursory. It explained, “[a]lthough we need not reach this issue, since we have already held plaintiffs have demonstrated a likelihood of success on their First Amendment argument, we do so, albeit briefly.”¹²⁰

The court of appeals agreed with the district court, finding that the statute violated the Commerce Clause in three respects. First, it regulated conduct occurring wholly outside New Mexico.¹²¹ Second, it constituted an unreasonable and undue burden on interstate and foreign commerce.¹²² Third, it subjected interstate use of the Internet to inconsistent state regulation.¹²³ In making this finding, the district court and the court of appeals relied exclusively on *American Libraries Ass’n v. Pataki*¹²⁴—the only applicable court decision to date.

In finding that the statute regulated conduct occurring outside the state, the court stated that section 30-37-3.2 contained no express limitation that confined it to communications occurring completely within its borders. “Rather, it ‘applie[d] to any communication, intrastate or interstate, that fits within the prohibition and over which [New Mexico] has the capacity to exercise criminal jurisdiction.’”¹²⁵ Further, even if the statute applied only to one-on-one e-mail communications, it would still fail Dormant Commerce Clause scrutiny as there is no way to guarantee that a communication from one New Mexican to another will not travel through other states en route. Like the *Pataki* court, the court of appeals concluded that section 30-37-3.2 does not and “cannot effectively be limited to purely intrastate communications over the Internet because no such communications exist.”¹²⁶ Mirroring the reasons discussed in *Pataki*, the court of appeals also agreed that under the *Pike* balancing test the burden the statute imposed on interstate commerce outweighed its local benefit.¹²⁷ While the protection of minors is a legitimate state interest, the statute would not be able legally to limit content coming in from other countries.

120. *Johnson*, 194 F.3d at 1160.

121. *See id.* at 1161.

122. *See id.* at 1162.

123. *See id.*

124. 969 F. Supp. 160 (S.D.N.Y. 1997).

125. *Johnson*, 194 F.3d at 1161 (quoting *Pataki*, 969 F. Supp. at 169–70) (second alteration in original).

126. *Id.* at 1161 (quoting *Pataki*, 969 F. Supp. at 171).

127. *See id.* at 1161–62.

The court again echoed the decision in *Pataki* by holding that the statute would violate the Dormant Commerce Clause by subjecting the Internet to inconsistent regulation.¹²⁸ The Supreme Court has long recognized that certain areas of commerce are uniquely suited to national, as opposed to state, regulation.¹²⁹ The court of appeals found that “[t]he Internet is surely such a medium.”¹³⁰

b. *California: how not to avoid Dormant Commerce Clause scrutiny*

Though no type of state regulation is impervious to a Dormant Commerce Clause attack, some state Internet regulations are more likely to withstand scrutiny than others. Section 288.2(b) of the California Penal Code, though very similar to the regulations discussed above, is unlike the New York and New Mexico statutes in that it requires a defendant to have knowledge of the fact that material is distributed to a minor.¹³¹ Section 288.2(b) states:

Every person who, with knowledge that a person is a minor, knowingly distributes . . . by electronic mail, the Internet . . . or a commercial online service, any harmful matter . . . to a minor with the intent of arousing, appealing to, or gratifying the lust or passions or sexual desires of that person or of a minor, and with the intent, or for the purpose of seducing a minor, is guilty of a public offense. . . .¹³²

According to this section, California cannot penalize an Internet user for *accidentally* sending harmful material to a minor. This knowledge requirement eliminates some of the statute’s burden on interstate commerce by not covering most types of Internet communications. In fact, just about the only time a user can be penalized by the California statute is when the sender has positive identification of a recipient’s age. But can this knowledge requirement offset enough of the statute’s burden on interstate commerce to overcome the grasp of the Dormant Commerce Clause?

Applying the *Pataki* formula suggests it cannot. First, with or without the knowledge requirement, section 288.2(b) regulates behavior occurring outside the state. There is no language in the text of the statute expressly limiting its reach to intrastate conduct. Even assuming such a limit, there would be no way to tell whether any particular out-of-state communication

128. *See id.* at 1162–63.

129. *See, e.g.,* *Wabash, St. Louis & Pac. Ry. v. Illinois*, 118 U.S. 557 (1886) (holding that states cannot regulate railroad rates).

130. *Johnson*, 194 F.3d at 1162.

131. CAL. PENAL CODE § 288.2(b) (West 1999).

132. *Id.*

had traveled through California.¹³³ A knowledge requirement has no effect on the ambit of an Internet transmission.

Second, although the knowledge requirement significantly reduces the burden on interstate commerce, it also reduces the benefit. It lessens the burden by not criminalizing out-of-state transmissions that are: (1) intended for other states and intercepted by minors in California; (2) intended for adults in California and intercepted by minors; and (3) made to another with no knowledge of the age of the recipient. This means people who publish out-of-state free-for-all pornographic web sites with no age verification need not concern themselves with section 288.2(b). In fact, the only out-of-state party that falls within the scope of the statute is one that broadcasts harmful material directly to a minor with knowledge that the recipient is a minor.

The knowledge requirement also reduces, and perhaps even eviscerates, the local benefit as well. In one-on-one communications, a knowledge requirement would not make California Internet broadcasters stop sending obscenity to minors, but instead would enable them to close their eyes to the identity of the recipients. Along the same lines, in transmissions to the entire Internet community, a pornographic California web page could evade the reach of the statute by simply choosing not to use age verification. The only in-state party that can be penalized by the statute is one that broadcasts harmful material directly to a minor with knowledge that the recipient is a minor. One must at this point remember to keep in mind the difficulty of tracking down the origin of an Internet transmission.¹³⁴ Thus, while the interstate commercial burden of the statute is only upon out-of-state Internet users who knowingly communicate harmful material to minors, the in-state benefit is limited to the protection of minors from harmful material knowingly transmitted to them on those rare occasions when those perpetrators can be found. The burden and benefit imposed by section 288.2(b) are far more equivalent than the burden and benefit imposed by the New York and New Mexico statutes.

The third *Pataki* consideration helps to resolve the problems caused by this burden-benefit equilibrium. Section 288.2(b), like the New York and New Mexico statutes, subjects the Internet to inconsistent regulations. Regardless of the mental state (knowledge) requirement, if all fifty states imposed legislation similar to section 288.2(b), Internet broadcasters would be forced to comply with each state's regulation before making any Internet

133. See *supra* text accompanying note 42.

134. See *supra* text accompanying notes 32–36.

communications. As the *Pataki* court held, the Internet is a unique area that requires the consistency of federal legislation.¹³⁵

Because the statute regulates commerce wholly outside California and would engender inconsistent Internet regulation, it is unlikely that it would withstand Dormant Commerce Clause muster. This analysis demonstrates that state statutes which directly regulate Internet communication are unlikely to survive Dormant Commerce Clause scrutiny regardless of how narrowly tailored they may be.

2. Gambling

In addition to the legal issues discussed in the context of obscenity, Internet gambling prohibitions raise many unique legal questions. To better understand these issues, one must first understand how Internet gambling operates. After users load an Internet gambling web page, they may be confronted with legal language advising consultation with the state's laws before proceeding.¹³⁶ The page may either refer users to a telephone number for their state, or simply allow them to gamble directly through the Internet. At this point, the site may require the user to open an account and make a minimum deposit before betting.¹³⁷ Gambling sites then ask the user for wired funds, money orders, or credit card cash advances to start an account.¹³⁸ After a short verification process, the user can start gambling.

Although the federal government can and does control gambling that affects interstate commerce,¹³⁹ states have traditionally been left to decide the extent to which gambling will be permitted within their borders.¹⁴⁰ While some states permit gambling,¹⁴¹ others have take intermediate approaches to the issue¹⁴² or prohibit gambling entirely.¹⁴³ But as of now,

135. *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 181–83 (S.D.N.Y. 1997).

136. See Comment, John Edmund Hogan, *World Wide Wager: The Feasibility of Internet Gambling Regulation*, 8 SETON HALL CONST. L.J. 815, 821–22 (1998).

137. See Steven Crist, *All Bets Are Off*, SPORTS ILLUSTRATED, Jan. 26, 1998, at 82, 90.

138. See *id.*

139. See Rory K. Little, *Myths and Principles of Federalization*, 46 HASTINGS L.J. 1029, 1062 n.154 (1995) (discussing *Champion v. Ames*, 188 U.S. 321, 357–58 (1903), which upheld a federal law criminalizing interstate transportation of lottery tickets, noting state power to forbid gambling).

140. See Jewel N. Klein & Ray H. Garrison, *Practice and Procedure Before Racing Commissions*, 78 KY. L.J. 477, 496 (1989–90).

141. See Thomas Lee Hazen, *Rational Investments, Speculation, or Gambling?—Derivative Securities and Financial Futures and Their Effect on the Underlying Capital Markets*, 86 NW. U. L. REV. 987, 1004 n.92 (1992) (recounting the legalization of gambling in Nevada).

142. See Edward J. McCaffery, *Why People Play Lotteries and Why It Matters*, 1994 WIS. L. REV. 71, 72 (1994) (noting that gambling is permitted through state-sponsored and operated lotteries).

the question of whether a state may prohibit gambling *on the Internet* remains unanswered.¹⁴⁴

It is not relevant whether a gambling web site advises users situated in non-gambling states not to use the site to gamble. A user in Utah, while just as able to access such a web page, is also just as unlikely as a user in Nevada to heed the warnings of such advisories (perhaps even less likely).

To analyze whether state Internet gambling legislation can survive the Dormant Commerce Clause, we refer to section 90.3 of the portion of Louisiana's criminal code that addresses gambling. The statute reads:

Whoever designs, develops, manages, supervises, maintains, provides, or produces any computer services, computer system, computer network, computer software, or any server providing a Home Page, Web Site, or any other product accessing the Internet, World Wide Web, or any part thereof offering to any client for the primary purpose of the conducting as a business of any game, contest, lottery, or contrivance whereby a person risks the loss of anything of value in order to realize a profit shall be fined not more than twenty thousand dollars, or imprisoned with or without hard labor, for not more than five years, or both.¹⁴⁵

The Dormant Commerce Clause analysis for this gambling statute progresses in much the same manner as did the analysis for the obscenity laws. Before applying Dormant Commerce Clause scrutiny, there must be a finding that the act in question applies to interstate commerce. Like the New York obscenity law, it is clear that the Louisiana statute does not discriminate against interstate commerce on its face. Therefore, the law should not be examined with a presumption of a protectionist purpose, let alone be ascribed "per se invalidity."¹⁴⁶

As for the legislative intent behind the statute, subsection (A) of section 90.3 specifically addresses its avowed purposes. It states:

The Legislature of Louisiana, desiring to protect individual rights, while at the same time affording opportunity for the fullest development of the individual and promoting the health, safety, education, and welfare of the people, including the children of this state who are our most precious and valuable resource, finds that the state has a compelling interest in protecting its citizens and children from certain activities and influences

143. See Kevin J. Worthen & Wayne R. Farnsworth, *Who Will Control the Future of Indian Gaming? "A Few Pages of History is Worth a Volume of Logic"*, 1996 BYU L. REV. 407, 438 n.154 (1996) (noting total prohibition on gambling in Hawaii and Utah).

144. I was unable to find a single case dealing with a state prohibiting gambling on the Internet.

145. LA. REV. STAT. ANN. § 90.3(E) (West 1999).

146. See *supra* text accompanying note 67.

which can result in irreparable harm. The legislature has expressed its intent to develop a controlled well-regulated gaming industry. The legislature is also charged with the responsibility of protecting and assisting its citizens who suffer from compulsive or problem gaming behavior which can result from the increased availability of legalized gaming activities.¹⁴⁷

As far as the text of the statute reveals, the intent of the legislature was clearly not to burden interstate commerce. Rather, the text seems to indicate that the purpose of section 90.3 was to protect Louisiana citizens from the harmful results of gambling. Therefore, the Louisiana legislature was likely attempting to further a legitimate interest when it enacted the law. This is not dispositive, however; as the *Pataki* court stated, “[t]he conclusion that the Act must apply to interstate as well as intrastate communications receives . . . its strongest support from the nature of the Internet itself.”¹⁴⁸ Because of its distinctive features (e.g., packet switching, smart networking, relentless anonymity), the Internet is inherently an instrument of interstate commerce, and therefore, a law which prohibits Internet gambling unavoidably concerns interstate commerce.¹⁴⁹

The next step of the analysis is to question whether Louisiana’s anti-gambling act violates the dormant aspect of the Commerce Clause in that it unduly burdens interstate commerce. Judge Preska found in *American Libraries Ass’n v. Pataki* that the protection of children from obscenity and pedophilia on the Internet was by itself insufficient to overcome the quantitative burden the New York law would have imposed on interstate commerce.¹⁵⁰ Similarly, while Louisiana may have a legitimate interest in protecting its people from the injurious effects of gambling, this benefit, alone, is not sufficient to overcome the burden the statute imposes on interstate commerce. There are three simple reasons for this.

First, the benefit to be derived from the Act is very small. Like the New York obscenity law, an anti-gambling act cannot protect its citizens from gambling because it cannot stop gambling web sites located outside the United States. Moreover, both web sites as well as end users who are physically located within the borders of the anti-gambling state can make themselves appear as though they are located outside the anti-gambling state. There is also no way for a gambling web site located outside the state to know exactly where its registrants are located.

147. § 90.3(A).

148. *American Libraries Ass’n v. Pataki*, 969 F. Supp. 160, 170 (S.D.N.Y. 1997).

149. *See id.* at 173.

150. *Id.* at 178.

Second, the burden the Louisiana law would have on interstate commerce is potentially enormous. Operators of gambling web sites located in states where gambling is permitted would have to remove their sites or risk being held liable for unknowingly gambling with residents of non-gambling states. Because gambling information will inevitably pass through the physical confines of a non-gambling state, gambling web sites and their users who are gambling legally chance violating a non-gambling state's law. Like the New York law, this would have the effect of chilling online communication by scaring people off the Internet.¹⁵¹

Finally, the risk of inconsistent legislation must again be considered, as non-gambling states will likely have anti-gambling laws that vary in form and severity. This risk, coupled with the chilling effect of such legislation, will make enacting functional anti-Internet gambling legislation all but impossible.¹⁵² This analysis reveals the conclusion that state Internet gambling legislation will likely meet the same fate as the obscenity statutes discussed above. While states may regulate gambling within their geographical borders, they may not regulate gambling on the Internet.

3. *Unsolicited e-mail: tailoring a law to withstand Dormant Commerce Clause scrutiny*

Unsolicited electronic mail advertisements ("spam") occur when an Internet user sends some type of advertisement formatted for e-mail to a large list of e-mail addresses. These lists are typically purchased from companies that compile user information that has been entered into various Internet sites. Unwanted spam messages are annoying to the end user and have been blamed for large-scale Internet slow-downs. Though California enacted Business and Professions Code section 17538.45 to combat spam, the statute also serves as a good example of how a state law targeted directly at the Internet can be tailored narrowly enough to withstand Dormant Commerce Clause scrutiny. Section 17538.45(b) states:

No registered user of an electronic mail service provider shall use or cause to be used that electronic mail service provider's equipment located in this state in violation of that electronic mail service provider's

151. See *ACLU v. Reno*, 929 F. Supp 849, 863 (E.D. Pa. 1996) (holding that individuals, uncertain of the reach of the CDA, will undoubtedly "steer far wider of the unlawful zone").

152. See *Pataki*, 969 F. Supp at 176 ("while Congress could enact a law requiring full disclosure of every presale repair to an automobile, no single state could impose such a policy nationwide by imposing economic sanctions aimed at changing the conduct of a tortfeasor in other states") (citing *BMW of N. Am., Inc. v. Gore*, 517 U.S. 559 (1996)).

policy prohibiting or restricting the use of its service or equipment for the initiation of unsolicited electronic mail advertisements.¹⁵³

The likelihood of the California statute surviving the Dormant Commerce Clause depends largely on the definitions of the terms contained therein. The statute basically says, "No registered user of an electronic mail service provider shall use that . . . provider's equipment located in this state in violation of that provider's policy prohibiting [spam] . . ." ¹⁵⁴ Applying the Dormant Commerce Clause analysis to section 17538.45(b) would, at this point, produce a result similar to that for obscenity statutes.

First, as discussed above, nothing in the text of section 17538.45(b) limits its application to wholly intrastate actions. This is because an out-of-state spammer registered to a national electronic mail service provider can run afoul of the statute if he sends spam that is inadvertently routed through the provider's California equipment.¹⁵⁵ Second, the intended local benefit of the law is probably outweighed by the burden it imposes on interstate commerce. The California statute would burden interstate commerce by causing spammers (or any users scared of being characterized as spammers¹⁵⁶) located out-of-state and registered with a national e-mail service provider that also provides service in California to halt their operations. It would also criminally prohibit e-mailers located in California from violating their service providers' policies. In so doing, these same users would be criminally forbidden to send spam to anywhere outside the state via the equipment of their California e-mail service providers. However, it is not especially clear how much of a burden such a criminal penalty would impose in light of the contractual remedy the provider would have against its registrant.

The local benefit would be criminal restriction against California e-mailers' sending spam to California users in violation of their e-mail service providers' policies. Taking into account the difficulties of enforceability discussed earlier,¹⁵⁷ the balance seems to tip slightly in favor of the burden. When coupled with the fact that such a statute could open

153. CAL. BUS. & PROF. CODE § 17538.45(b) (West Supp. 2000).

154. *Id.*

155. This can be better explained by way of example. Sam Smith is a spammer registered to Earthlink. He lives in Ohio and receives his e-mail service from Earthlink's Ohio servers. If he sends spam to a New York AOL subscriber in violation of Earthlink's spam policies, and that mail happens to be routed through Earthlink's California equipment, he is subject to criminal penalties in California.

156. *See supra* text accompanying note 110.

157. *See supra* text accompanying note 105.

the door to inconsistent Internet regulation, it seems likely that section 17538.45(b) would violate the Dormant Commerce Clause.

“Initiation,” however, is defined under section 17538.45(a)(2)(B)(4) as “[an] action by the initial sender of the electronic mail advertisement. It does not refer to the actions of any intervening electronic mail service provider that may handle or retransmit the electronic message.”¹⁵⁸ This highlights the importance of definitions. This changes the statute to read, “No registered user of an electronic mail service provider shall use . . . that provider’s equipment located in this state in violation of that . . . provider’s policy . . . prohibiting [spam] . . . for the *initiation* of [spam].”¹⁵⁹ This qualification limits the scope of the statute to spam that is initiated in the California equipment of an e-mail service provider. As a result, there is no effect on an out-of-state spammer registered to a national electronic mail service provider who sends spam that is inadvertently routed through the provider’s California equipment. This lessens the burden on interstate commerce in two ways. First, the out-of-state spammer need not concern himself with California’s law. Second, this eliminates the problem of inconsistent legislation.

The definitional modification, however, does not completely eliminate the burden. What remains is the criminal penalty imposed on California users who wish to send spam outside the state. But, as discussed above, this burden is minimal considering that (1) it only applies when users violate their providers’ policies, and (2) violation of providers’ policies would be subject to civil remedy regardless of the existence of the statute. Considering the minimal remaining burden on interstate commerce, and the now absent risk of inconsistent legislation, section 17538.45(b) would probably not violate the Dormant Commerce Clause.

Though the initiation limitation helps section 17538.45(b) withstand constitutional muster, it also substantially diminishes the law’s value. Once the statute is read to include the limitation, its ambit of application is reduced to include only Internet users who send spam from California. Section 17538.45(b) does nothing to protect California users from spam originating outside the state. Thus, when a state attempts constitutionally to regulate Internet communications, the result will almost inevitably be a gutted, ineffective law.

158. § 17538.45(a)(2)(B)(4).

159. § 17538.45(b) (emphasis added).

B. REGULATION OF CONTRACTS AND TRANSACTIONS

1. *Digital signatures*

Because an Internet transmission is not a writing,¹⁶⁰ it cannot satisfy the traditional statute of frauds writing and signature requirements. Digital signatures solve this problem by carrying out two functions: (1) they authenticate documents, and (2) they make documents non-repudiable.¹⁶¹ A digital signature is an electronic substitute for a handwritten signature that serves the same basic functions while providing an extra level of security. Thus, “[it] is an arcane term for an encoded message that assures each party in an electronic transaction that the other party is who they [sic] say they are. . . . [And it] assures that a received message is valid, remaining unchanged from the point and time of delivery.”¹⁶² If a recipient of a digitally signed document can verify the sender’s digital signature, the recipient can verify the validity of the document, because the digital signature can authenticate both the sender’s identity and the content contained in the transmission.¹⁶³

Because electronic transmissions generally can be undetectably altered or copied, proof of the legitimacy of these transmissions is required.¹⁶⁴ The digital signature solves this problem by encrypting and decrypting information through the use of two keys: a private key that only the signer should know, and a public key which is made openly available through storage in a public database. The result of this key encoding is a long and unintelligible string of alphanumeric characters that bear absolutely no resemblance to a traditional signature. Because this encoding cannot be identified and replicated by a third party, digitally signed documents cannot be undetectably altered.

In order for a digital signature to be worthwhile, the receiver of a digitally signed transmission needs to consult a “trusted third party” to

160. By this I mean that an Internet transmission is not a writing within the traditional sense and meaning of the term.

161. See Raymond T. Nimmer, *Information Age in Law: New Frontiers in Property and Contract*, N.Y. ST. B.J., May–June 1996, at 28, 31.

162. Brian W. Smith & Timothy E. Keehan, *Digital Signatures: The State of the Art and the Law*, 114 BANKING L. J. 506, 507 (1997).

163. See John P. Tomaszewski, Comment, *The Pandora’s Box of Cyberspace: State Regulation of Digital Signatures and the Dormant Commerce Clause*, 33 GONZ. L. REV. 417, 421 n.30 (1997–98).

164. See Martin E. Hellman, *Implications of Encryption Policy on the National Information Infrastructure*, COMPUTER L., Feb. 1994, at 28, 31.

validate the signature.¹⁶⁵ This “trusted third party,” known as the Certification Authority (“CA”), is consulted whenever a digital signature is attached to a document to verify its integrity. The CA functions very much like a conventional notary public.¹⁶⁶ “Without the use of CAs, electronic commerce has no ready means of generating legitimate digital signatures for online contracting.”¹⁶⁷

As of 1999, more than forty states had already enacted laws regarding the use of digital signatures and CAs.¹⁶⁸ Similar legislation has been considered in almost every state.¹⁶⁹ Two paradigms of digital signature legislation have been followed.

The first type imposes regulations on Internet transactions where the state is a market participant but imposes no regulations upon digital signature transactions where the state is not a party to the contract. In essence, these laws state that (1) *any* type of digital verification contracting parties choose to use for Internet transactions is binding on those parties, and (2) the state will only accept certain digital verification methods when it is contracting with another party (acting as a market participant). For example, section 09.25.510 of the Alaska Code of Civil Procedure states only that “a state agency or political subdivision[] may accept or agree to be bound by an electronic record executed or adopted with an electronic signature,”¹⁷⁰ without actually limiting the acceptable forms of digital verification procedures. Massachusetts’ regime is more restrictive as it lists only a few types of electronic signature verification formats it will accept when the State is a party to an Internet transaction.¹⁷¹ For contracts in which the state is not a market participant, section 09.25.510 of the Alaska Code of Civil Procedure states only that “[w]here a person accepts or agrees to be bound by an electronic record executed or adopted with an

165. See, e.g., Richard L. Field, *Survey, 1996: Survey of the Year’s Developments in Electronic Cash Law and the Laws Affecting Electronic Banking in the United States*, 46 AM. U. L. REV. 967, 985 (1997).

166. See 58 AM. JUR. 2D *Notaries Public* § 1 (1989) (“A notary public is defined as a[n] . . . impartial agent of the state . . . [who attests to] the genuineness of any deals or writing . . . and . . . the authenticity of signatures.”).

167. Tomaszewski, *supra* note 163, at 435.

168. See Kalana M. Lui-Kwan, *Digital Signatures: Recent Developments in Digital Signature Legislation and Electronic Commerce*, 14 BERKELEY TECH. L.J. 463, 472 (1999). Several states, including Georgia, West Virginia, Iowa, New Hampshire, Wisconsin, Kansas, Arkansas, South Dakota, Minnesota, Nebraska, Kentucky, Oregon, and Illinois, have enacted far-reaching legislation in this area. See *id.*

169. See *id.*

170. ALASKA CODE CIV. PROC. § 09.25.510.

171. See *MERSA* § 4 (April 14, 1998) <<http://www.magnet.state.ma.us/itd/legal/mersa.htm>> [hereinafter *MERSA*] (draft of Massachusetts Electronic Records and Signatures Act).

electronic signature, a rule of law that requires (1) a record of that type to be in writing shall be considered satisfied; and (2) a signature shall be considered satisfied."¹⁷² Massachusetts recognizes *any* type of electronic means of writing and signing that the contracting businesses themselves agree to as valid and binding on the parties.¹⁷³

The second type of digital signature legislation imposes far more restrictions on the negotiating parties¹⁷⁴ as it defines the duties, liabilities and standards for private and public CAs.¹⁷⁵ This puts the state in the position of the market regulator,¹⁷⁶ rather than the market participant.¹⁷⁷ The problem with this paradigm is quite clear—while a CA's license and certification may be recognized under one state's statutory framework, a CA that is licensed under a different framework (i.e., the Massachusetts model) may not be acceptable.¹⁷⁸ This means a CA could be invalid in a state if it does not follow that state's licensing scheme. With no pen-signed paper original to fall back on, this would subject the digitally signed documents to the vague, time consuming, costly, and litigation-intensive rules of evidence.

The first type of state legislation, the Massachusetts/Alaska paradigm, would likely pass Dormant Commerce Clause scrutiny. As discussed above, the market participant exception to the Dormant Commerce Clause gives the state the right to enact legislation that might ordinarily impose an excessive burden on interstate commerce so long as the state is a party to the transaction.¹⁷⁹ Like the law at issue in *Reeves Inc. v. Stake*,¹⁸⁰ this type of legislation only makes use of the state's right to contract freely. As long as the state does not try to control anything other than the transaction to which it is a party,¹⁸¹ there is no bar to the law.

The parts of the Alaska and Massachusetts statutes that do not fall within the purview of the market participant exception would pass Dormant Commerce Clause scrutiny as well. The second part of the Massachusetts

172. § 09.25.510.

173. See *MERSA*, *supra* note 171, § 3.

174. For more information on this second type of regulation see Thomas G. Mellig, *Washington's Electronic Authentication Act: Eliminating Legal Uncertainties Through Default Rules*, 34 SAN DIEGO L. REV. 1247 (1997).

175. See WASH. REV. CODE ANN. §§ 19.34.010–.903 (West Supp. 1998).

176. See *supra* text accompanying notes 78–80.

177. See generally JOHN E. NOWAK & RONALD D. ROTUNDA, CONSTITUTIONAL LAW § 8.9 at 306–08 (5th ed. 1995).

178. See § 19.34.100(5).

179. See *supra* text accompanying note 78.

180. 447 U.S. 429 (1980).

181. See *supra* text accompanying note 80.

statute states, “[a] contract between business entities shall not be unenforceable, nor inadmissible in evidence, on the sole ground that the contract is evidenced by an electronic record or that it has been signed with an electronic signature.”¹⁸² Likewise, the Alaska statute states that when parties agree to be bound by a digital signature, “a record of that type . . . in writing shall be considered satisfied,” and “a signature shall be considered satisfied.”¹⁸³

Because neither of these statutes discriminates against interstate commerce on its terms, both statutes are to be analyzed without a presumption of a protectionist purpose, weighing the quantitative burden on interstate commerce imposed by the law against the putative local benefit.¹⁸⁴ Because neither law restricts the usage or form of digital signatures, neither regulates what kind of CAs can be used, how CAs may be used, or the purposes for which CAs may be used. Rather, the laws allow those conducting transactions on the Internet to choose their desired means of verification. In so doing, they actually benefit interstate commerce by allowing certain Internet transactions to be enforceable when they otherwise would not be. At the same time, these statutes impose almost no burden on interstate commerce.

The more burdensome type of digital signature law, however, presents a more involved Dormant Commerce Clause question. A state which has enacted this second type of law basically declares that if a CA wishes to be the “trusted third party” in transactions within that state, it must follow that state’s guidelines or even be licensed by that state.¹⁸⁵ Because the law of contract formation traditionally has been left to the state, this does not appear to be a problem. But upon closer scrutiny, the application of this legal tradition is inappropriate. State controls of contract law usually affect only the intrastate performance or formation of contracts. A burdensome CA law, on the other hand, directly exerts its influence on the law-making ability of all states, because CAs licensed elsewhere would have to follow the more burdensome state’s regulations. The Supreme Court has made it clear that such regulations are subject to Dormant Commerce Clause scrutiny.¹⁸⁶

The next question is whether the burdensome type of CA regulation can withstand Dormant Commerce Clause analysis. First, so long as these

182. See *MERSA*, *supra* note 171, § 5.

183. ALASKA CODE CIV. PROC. § 09.25.510(1)–(2).

184. See *supra* text accompanying notes 58–72.

185. See WASH. REV. CODE ANN. § 19.34.100 (West Supp. 1998).

186. See *supra* note 77 and accompanying text.

statutes do not discriminate against interstate commerce by their terms, they should not be presumed protectionist. Even assuming such discrimination, the legitimate state interest in maintaining the integrity of Internet transactions would help to dissipate any resulting presumption of protectionism.¹⁸⁷ There are, however, several less burdensome alternatives to these statutes.¹⁸⁸ First, a simple alternative exists in recognizing all CAs that have already been accepted by other states. Second, a myriad of private and national government organizations exist today which approve CAs.¹⁸⁹ A state could simply demand that a CA be accredited by a national CA accreditation facility, thereby alleviating any risk of inconsistent legislation.

Given the less burdensome alternatives, we end our analysis with an inquiry into whether the residual quantitative burden imposed by the law is excessive in light of the putative local benefit. These laws provide the benefit of a state standard for CAs, and to a large extent, regularity, dependability, and integrity. But even this significant local benefit is not decisive here because less burdensome alternatives also exist. This is especially true considering that the burden imposed by this legislation is significant. Such laws make themselves a *de facto* national standard by forcing every CA wishing to do business within a state to get licensing from that state. Worse yet, if two states were to have differing licensing schemes, CAs would be prohibited from doing business in both states. These laws have the potential to be destructive to the very industry they have been enacted to protect. For these reasons, it is unlikely that this more burdensome species of digital signature state laws could pass constitutional muster.

2. *Nondata-type Internet transactions*

Another type of state law susceptible to Dormant Commerce Clause scrutiny is the regulation of nondata Internet transactions. The nondata¹⁹⁰ category of Internet transaction basically uses the Internet as a highly

187. See *supra* note 73 and accompanying text.

188. See *supra* text accompanying note 74 (noting that the Supreme Court has, in the past, allowed the use of facially discriminatory statutes where there is no less burdensome alternative to advancing the legitimate state interest).

189. See *MA.US/ITD/LEGAL* (visited Jan. 29, 1999) <<http://www.state.ma.us/itd/legal>> (Information Technology Division homepage for the Commonwealth of Massachusetts, discussing uniform CA rating guidelines being developed by several states in collaboration with the federal government).

190. When I use the term "nondata," I do not mean that no data is being exchanged. I only mean that the good being transferred from seller to buyer is physical and tangible rather than data-type content.

sophisticated mail order catalog.¹⁹¹ Shoppers use advanced interactive web pages to browse through companies' product line-ups instead of dealing with clunky magazines, long hold times, and rude and unhelpful telephone salespeople. When they find the product they want at an acceptable price, they can purchase it online and expect it to find it at their doorstep a few days later. To date, no state regulation of this type of Internet transaction has been tested on Dormant Commerce Clause grounds, but in certain situations, state regulations of Internet transactions dealing with physical goods would assuredly meet with failure.

There are two types of nondata Internet transaction regulation. The first type either regulates the sale of certain kinds of goods or prohibits the sale of those goods altogether. For example, consider a Minnesota law that bans all retail sale to persons in Minnesota (whether conducted on the Internet or not) of milk products in plastic nonreturnable containers but permits all retail sale to persons in Minnesota of milk products in glass nonreturnable containers.¹⁹² At first glance, this law seems to have the same problem as the New York obscenity law—under certain conditions it prohibits the movement of certain material into the state.¹⁹³ Yet closer observation leads to a different outcome.

Applying Dormant Commerce Clause scrutiny to the Minnesota law reveals the following: (1) the law is not discriminatory on its face—it regulates even-handedly by treating milk products originating inside the state just like it treats milk products originating outside the state, and (2) the legitimate state interest in the law, according to the legislature, was to combat a waste management problem. However, a better plastic processing system of some sort could be an alternative less burdensome to interstate commerce.

The real difference between the Minnesota and New York laws comes in balancing the local benefits against the burden on interstate commerce. The benefit is a partial solution to the state's waste management problem. Yet unlike the New York obscenity law, the Minnesota law's burden does not depend upon the nature of the Internet itself. Because all transactions of physical goods require knowledge of a physical, geographical shipping destination, the Minnesota law would *only* affect, and therefore *only* bar, transactions by which milk is shipped to persons in Minnesota. The

191. See Dan L. Burk, *Trademark Doctrines for Global Electronic Commerce*, 49 S.C. L. REV. 695, 702 (1998).

192. See *Minnesota v. Clover Leaf Creamery Co.*, 449 U.S. 456 (1981). The law considered here is an alteration of the Minnesota statute at issue in *Clover Leaf*.

193. See *supra* text accompanying notes 85–93.

idiosyncrasies of the Internet do not apply. The Internet characteristic of this law adds no burden to the Dormant Commerce Clause equation, leading to the conclusion that all Internet laws of this type are no more burdensome than their non-Internet counterparts. They can similarly withstand Dormant Commerce Clause scrutiny.¹⁹⁴

For an example of a state law that regulates (rather than prohibits) the sale of goods over the Internet, consider a slightly modified version¹⁹⁵ of California Business and Professions Code section 17538(d). The law states, in part:

A vendor conducting business through the Internet or any other electronic means of communication shall do . . . the following when the transaction [involving the sale of physical goods] involves a buyer located in California: . . . [b]efore accepting any payment or processing any debit or credit charge or funds transfer, the vendor shall disclose to the buyer in writing or by electronic means of communication, such as E-mail or an on-screen notice, the vendor's return and refund policy, the legal name under which the business is conducted and . . . the complete street address from which the business is actually conducted.¹⁹⁶

Like the Minnesota law discussed above, section 17538(d) would probably not offend the Dormant Commerce Clause. First, section 17538(d) does not discriminate against out-of-state sellers by its terms. No provision in the statute references out-of-state Internet vendors but not in-state Internet vendors. Second, there is a legitimate local interest in enacting the law, namely, consumer protection. Third, there are probably no less-discriminatory alternatives that could provide for as much convenient information disclosure. Balancing the interstate burdens of the law against the in-state benefits also works out in favor of section 17538(d). Unlike the obscenity laws discussed previously, the burden does not depend upon the nature of the Internet itself because section 17538(d) only applies when an Internet seller is aware of the geographical location of the buyer; the law only applies to sales involving California buyers.

194. See *Hughes v. Oklahoma*, 441 U.S. 322 (1979) (holding unconstitutional an Oklahoma law that prohibited people from transporting or shipping minnows for sale outside the state because it placed no barriers on the numbers of minnows that could be appropriated by licensed intrastate minnow dealers and did not limit disposition of minnows within the state).

195. See *infra* text accompanying note 207. I added the phrase, "involving the sale of physical goods" into the law for analytical purposes. The real law makes no distinction between transactions involving the sale of physical goods and transactions involving the sale of data goods. As will be seen in the following subsection, this distinction is critical because a law like section 17538(d) that only applies to physical goods is less likely to be violative of the Dormant Commerce Clause than a law that ignores this distinction.

196. CAL. BUS. & PROF. CODE § 17538(d) (West 1999).

Therefore, there is no burden on interstate commerce and likewise no risk of inconsistent legislation. Once the Internet vendor discovers that a buyer is geographically situated outside the state, the vendor can ignore the California law altogether. Like the Minnesota statute, section 17538(d) would not be invalidated by the Dormant Commerce Clause. The Minnesota and California statutes teach a simple lesson: When a state law regulates the sale of nondata goods, the application of that law to the Internet alone will not cause it to violate the Dormant Commerce Clause so long as the law would otherwise withstand Dormant Commerce Clause scrutiny.

The second type of regulation of physical goods targets the form or content of the web sites, e-mails or other Internet communications used to sell the goods. These regulations include laws that demand the use of specific types of encryption¹⁹⁷ on certain sites, call for the use of a minimum font size on mail-order web pages, and require the disclosure of certain information before sales takes place. Because such regulation is aimed at the Internet itself, the geographical location of a buyer is of no consequence, making this family of statutes more susceptible to a Dormant Commerce Clause attack.¹⁹⁸ Whenever a statute regulates the type or manner of content one may display on a web page, that statute confronts the same problems as did the New York obscenity law.¹⁹⁹

Another portion of California Business and Professions Code section 17538(d) exhibits this principle. Section 17538(d)(2) states, in part:

If the disclosure of the vendor's legal name and address information required by this subdivision is made by on-screen notice, all of the following shall apply:

(A) The disclosure of the legal name and address information shall appear on any of the following: (i) the first screen displayed when the vendor's electronic site is accessed, (ii) on the screen on which goods or services are first offered. . . .

(B) The disclosure of the legal name and address information shall be accompanied by an adjacent statement describing how the buyer may receive the information at the buyer's E-mail address.²⁰⁰

197. Encryption types, such as 128-bit strong encryption, put web page communications into code, enabling users to make secure transactions in online banking, stock trading and credit card sales.

198. Note that such statutes could run into significant First Amendment barriers as well, as they are, in a sense, regulating speech.

199. See *supra* Part II.B.

200. § 17538(d)(2).

This section requires a vendor to disclose information in certain places on the web site if a product is to be legally sold in California. Though section 17538(d)(2) does not discriminate against interstate commerce on its terms, it does in effect regulate commerce outside the state. The question is whether doing so levies an excessive or disproportionate impact on interstate commerce. As explained above,²⁰¹ section 17538(d)(2) inflicts a disproportionate impact because it applies solely to the Internet. In order to do business in California, all web pages selling merchandise must comply with the section. Because there is no way for the operator of a web page to make displayed content accessible in California and yet inaccessible in other states, California's Business and Professions Code is a *de facto* national standard. Section 17538(d)(2) is, in fact, so burdensome that if two states were to require the disclosure of contradictory information in the same location on a web page, vendors would not be able to do business in either state. The Supreme Court has specifically stated that those aspects of commerce that require consistent treatment may not be regulated by the states.²⁰²

As with most laws of this type, less restrictive alternatives do exist. The state could leave it to the market to choose which level and type of encryption is appropriate to a given situation.²⁰³ California could also make the law less burdensome by providing more general requirements. For example, a law could mandate only that certain information must be disclosed, rather than dictate where that information need be disclosed. Of course, the less specific the law is, the more dollars will be spent in term-defining litigation. Nevertheless, when this enervated state interest is balanced against the staggering encumbrance on interstate commerce, it becomes quite clear that these types of laws cannot, and almost certainly will not, withstand Dormant Commerce Clause muster.

201. See *supra* text accompanying notes 197–199.

202. See *supra* note 77 and accompanying text.

203. A look at an assortment of financial and other web pages demonstrates that the market has deemed different levels of encryption to be appropriate under different circumstances. See, e.g., [*Tell Me More*] – *Ameritrade, Inc.* (visited Oct. 3, 2000) <http://www.ameritrade.com/tell_me_more/> (128-bit Secure Socket Layer (SSL) encryption); *Welcome to Bank of America – Privacy Practices* (visited October 3, 2000) <<http://www.bofa.com/privacy/>> (SSL encryption); *E*TRADE* (visited Oct. 3, 2000) <<http://www.etrade.com>> (recommending users upgrade their web-browsing software to support available 128-bit encryption technology); *Fidelity Investments* (visited Oct. 3, 2000) <<http://www.fidelity.com>> (customers may choose either 40-bit or 128-bit encryption, depending on their web-browsing software capabilities); *Security on the Internet* (visited Oct. 3, 2000) <<http://www.wellsfargo.com/per/services/security/distributed/internet/>> (providing 128-bit encryption to all users by encrypting on its banking servers); *Yahoo! Privacy* (visited Oct. 3, 2000) <<http://privacy.yahoo.com/privacy/us/>> (SSL encryption used in certain areas).

3. *Data-type Internet transactions*

The second category of Internet sales involves traffic in digitized goods such as music, data, software and movies. Because customers can select, order, pay for, and receive these informational goods online, this type of commerce raises new and difficult legal questions. Regulations on the selection, ordering, and payment of goods via the Internet have been discussed above.²⁰⁴ What distinguishes this type of transaction from nondata Internet transactions is the ability to use the Internet to transfer the goods themselves. This calls into question whether states can theoretically or constitutionally prohibit or regulate the sale of certain goods over the Internet. Consider “the publication of a book that claimed that, toward the end of his life, former French President Francois Mitterand was unable to exercise the functions of his office.”²⁰⁵ A court order prohibited the book from being disseminated, and yet the book appeared for sale on the Internet shortly thereafter.²⁰⁶ The question is whether it is possible for a state to prohibit the sale of this book on the Internet without violating the dormant aspect of the Commerce Clause. The answer is almost certainly no.

For a Dormant Commerce Clause analysis of this very issue, consider again section 17358(d) of the California Business and Professions Code, only without any modifications.²⁰⁷ The unmodified law states:

A vendor conducting business through the Internet or any other electronic means of communication shall do . . . the following when the transaction involves a buyer located in California: . . . [b]efore accepting any payment or processing any debit or credit charge or funds transfer, the vendor shall disclose to the buyer in writing or by electronic means of communication, such as E-mail or an on-screen notice, the vendor’s return and refund policy, the legal name under which the business is conducted and . . . the complete street address from which the business is actually conducted.²⁰⁸

The difference between this law and those that apply exclusively to nondata type transactions is that this law applies to a product that is *itself* being transferred over the Internet (as opposed to the mere selection of

204. See *supra* Part III.B.2.

205. Geist, *supra* note 26, at 566. See Jane C. Ginsburg, *Copyright Without Borders? Choice of Forum and Choice of Law for Copyright Infringement in Cyberspace*, 15 CARDOZO ARTS & ENT. L.J. 153, 153 (1997).

206. See Geist, *supra* note 205.

207. See *supra* note 195 and accompanying text.

208. CAL. BUS. & PROF. CODE § 17538(d) (West 1999). Note that the unmodified version of the law makes no distinction between the sale of physical and nonphysical goods.

goods and payment over the Internet). Once we start dealing with Internet transfers of data products, the interstate aspects of Internet commerce are reintroduced into the equation. No longer does the physical address of the buyer limit the application of a state's law, because in many cases it simply is not known. The problem, again, is that a seller has no way of knowing to whom the product is being sold.²⁰⁹ To regulate the sale of a product sold to a buyer located in California, the seller must (1) implement credit-card-only sales with address verification, and (2) regulate all sales to follow the California law, or risk facing this state's penalties.

The argument structure proceeds as follows. As discussed above, section 17538(d) does not discriminate against out-of-state interests by its terms, but does regulate interstate commerce in its effect. Due to the nature of Internet data sales, there is probably no less-burdensome alternative. This leaves only a balancing of the residual quantitative burden imposed by the law against the putative local benefit. Basically, in order to avoid violating the law, all commercial web sites selling data goods over the Internet would either have to employ some kind of credit card address verification or comply with the law nationwide.

This burden is lower than that imposed by the obscenity laws discussed above. In *American Libraries Ass'n v. Pataki*,²¹⁰ the burden imposed on interstate commerce was that all communications dealing with obscenity, both commercial and noncommercial alike, would either have to cease entirely or implement some kind of credit-card-based or other form of age verification. The encumbrance imposed on interstate commerce here, however, is only that *commercial* web sites would have to shut down, comply, or implement credit card address verification. Ostensibly, requiring credit card address verification on only commercial Internet sites imposes a lesser burden than requiring credit card verification on all commercial *and* noncommercial sites. The effect is even lower considering the fact that most commercial sites already employ credit card verification to facilitate their sales. Noncommercial sites, on the other hand, would be forced to use credit card verification solely to satisfy the law. Though this statute imposes a lesser burden than the New York obscenity law, it is still significant, especially when considering the risk of inconsistent legislation. Therefore, such laws, because they force out-of-state Internet data sales companies to choose between conforming nationwide, employing credit

209. See *supra* text accompanying notes 32–36.

210. 969 F. Supp. 160 (S.D.N.Y. 1997).

card address verification, and shutting down, would be offensive to the Dormant Commerce Clause.

IV. REGULATION OF INTERNET SERVICE PROVIDERS: THE LEAST BURDENSOME ALTERNATIVE

An Internet Service Provider (“ISP”) is a company that sells Internet access to a group of subscribers via modem or direct connection. ISPs can also provide e-mail accounts, hosting and storage space for user web pages, newsgroup access, and a variety of other Internet functions. Certain ISPs, such as America Online (which are referred to as “online services”), provide various other proprietary features for subscribers independent of those available through the Internet. Some ISPs are regional in scope, while others, such as AT&T Worldnet and Earthlink, enjoy a national customer base. ISPs are essential to the functioning of the Internet as it exists today because they provide the link between most users and the Internet itself.

The role of ISPs in the fight against obscenity on the Internet has been discussed many times in the past.²¹¹ ISPs have the ability to use sophisticated screening software to filter various types of content from their subscribers. For example, when customers subscribe to America Online,²¹² they are provided with a number of different “screen names”²¹³ and passwords. Each family member in a household may receive his or her own unique screen name. Parents who subscribe to America Online are then provided with the option of filtering out undesirable pornographic content.²¹⁴ States have never required ISPs to employ or even offer such software. Rather, they have chosen to punish those who send obscenity after it has already been sent. Given that these criminal remedies will not pass Constitutional muster,²¹⁵ the question is whether states will be able to pass laws requiring ISPs to provide filtration options to their users without entering the domain of federal power.

A state law mandating that all ISPs providing service within the state offer obscenity filtration software of some kind to their subscribers would easily withstand Dormant Commerce Clause scrutiny. Because such a law only regulates ISPs doing business and providing service within the state, it

211. See, e.g., *Reno v. ACLU*, 521 U.S. 844, 850–57 (1997).

212. See *Welcome to AOL.COM* (visited Feb. 15, 1999) <<http://www.aol.com>>.

213. “Screen name” is America Online’s term for a username or login.

214. America Online even gives parents the right to remove e-mail access from their children’s accounts.

215. See *supra* Parts II.B, III.A.

imposes no more burden on interstate commerce than would any existing state business regulation. In fact, such a law would impose an even lower burden on interstate commerce than the nondiscriminatory nondata-type regulations discussed above.²¹⁶ ISPs doing business within the regulating state would have to obey that state's law, while out-of-state ISPs not doing business within the regulating state could ignore the law. Because these laws do not regulate business activity on the Internet as a whole, the inherent interstate characteristics of the Internet need not even be calculated into the equation.

While regulating ISPs cannot solve every Dormant Commerce Clause problem, it is a less burdensome alternative than criminal obscenity statutes. States such as Arizona²¹⁷ and South Dakota²¹⁸ have enacted legislation requiring public schools and libraries that provide public computer access to minors to equip those computers with filtration software. Yet despite the recommendations of Judge Preska²¹⁹ and the Supreme Court of the United States,²²⁰ no states have used the unique position of the ISP to block harmful Internet content from reaching minors. Because a law requiring ISPs to provide filtration devices would enable parents to choose the content their children receive, such a law would likely be more effective and less restrictive than criminal obscenity legislation. More important, because such a law raises fewer Dormant Commerce Clause issues, it has a better chance of survival. Why, then, have state legislatures chosen not to regulate ISPs? Perhaps they believe that the government's job is to control the flow of content on the Internet. Or perhaps they are failing to see the forest for the trees—by choosing only to punish the purveyors of obscenity, they are losing sight of the purpose of the legislation.

CONCLUSION

The applicability of the Dormant Commerce Clause has been forever broadened by the rise of the Internet. No longer will it be a concept learned in law school and forgotten thereafter. It will serve to limit the attempts of most states to regulate the Internet and related activities in a number of ways.

216. See *supra* Part III.B.2.

217. See ARIZ. REV. STAT. ANN. § 34-502 (West 1999).

218. See S.D. CODIFIED LAWS § 22-24-55 (Michie 1999).

219. See *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 180 (S.D.N.Y. 1997).

220. See *Reno v. ACLU*, 521 U.S. 844, 854-57 (1997).

Because the Internet is by its nature a facilitator of interstate commerce, the ability of the states to criminalize actions on the Internet will be significantly hampered by the Dormant Commerce Clause. States will generally be unable directly to regulate Internet-related operations, such as the licensing of Certification Authorities, because of the impact such legislation will have on national commercial activities. In most cases, it is also probably not within the states' power to regulate the form or content of web sites, regardless of the good being sold.

However, state regulations on certain types of Internet transactions may survive Dormant Commerce Clause scrutiny. Because certain nondata transactions involve tangible, and thus trackable, goods being delivered to a physical location, state prohibitions on Internet sales of goods being shipped into or within the state will likely not offend the Dormant Commerce Clause. More importantly, because regulating Internet Service Providers is inherently less burdensome than regulating Internet communications, such regulation will often be available as a solution to the Dormant Commerce Clause problem.

Because the Internet is evolving at an unprecedented pace, it is difficult to predict where or when state regulations will intercede next. But regardless of the ultimate outcomes, the Dormant Commerce Clause tools that date back to 1824 will grow and mature in the foreseeable future.